

Claims

1. A method of sending streamed data over an IP network from a first node to a second node, the method comprising:
 - using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes;
 - using the IKE SA to establish an IPSec SA between the first and second nodes;
 - encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPSec SA;
 - constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and
 - sending the IP datagrams from the first node to the second node.
2. A method according to claim 1, wherein said streamed data is VoIP data or videoconferencing data.
3. A method according to claim 1, wherein said peer nodes are end points for the data.
4. A method according to claim 1, wherein said peer nodes tunnel data between respective end points.
5. Apparatus for sending streamed data over an IP network to a peer node, the apparatus comprising:
 - processing means and memory containing software instructions for implementing IPSec protocols;
 - an application for delivering streamed data;
 - means for employing components of said processing means and memory containing software instructions for using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes;
 - means for using the IKE SA to establish an IPSec SA between the first and second nodes, the IKE SA comprising a shared secret;

6. Apparatus according to claim 5, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC).
7. Apparatus according to claim 6, the apparatus being a firewall or gateway coupled to an end point which is the source of the streamed data.